Maritime Domain Awareness

Technology is the easy part.

by Mr. Guy Thomas
Science & Technology Advisor, U.S. Coast Guard

Maritime Domain Awareness (MDA) has always been a focus for the U.S. Navy and U.S. Coast Guard, but, since September 11, 2001, the term has taken on new meaning as the sea services have worked to close security gaps in U.S. maritime frontiers. In the multi-front war against global terrorism, those who would exploit the maritime environment and transportation systems for unlawful or hostile means must be denied. U.S. national interests lie well beyond territorial waters and cannot be constrained by geographic boundaries. The United States is the world's leading maritime nation, whether measured by the sheer number of vessels plying its waters, the volume of goods transported by ship, or the economic value of its maritime commerce. With such reliance on an efficient and effective global maritime transportation system, the United States must be firmly committed to its security.

From the U.S. perspective, the sooner illegitimate activity in the global maritime environment can be identified and halted, the more secure the homeland will be. This means becoming aware of illegal or potentially threatening activities as distant from U.S. shores as possible to determine the optimal response. Taking that a step further, then, critical areas such as cargo loading facilities, embarkation/debarkation points, shipping lanes, choke points, as well as our own maritime approaches and facilities, must be monitored to establish a layered security regime. Additionally, layers of awareness must also be established that are centered upon traditional areas of interest, such as an environmental pollution and recovery, resource poaching, humanitarian efforts, or search and rescue operations.

Senior government officials, tasked with creating a national plan to improve Maritime Domain Awareness (see sidebar), recognized the need for the development of a common operational picture, with a user definable interface to a collaborative information environment (CIE). The challenge is to provide this common operational picture to all necessary entities in as complete and accurate manner as near to real time as possible. To do this, the envisioned collaborative virtual database must be equipped with the latest automated data manipulation tools, capable of data mining, pattern recognition, anomaly detection and other planner, analyst, and operator automated assistance tools.

The strategy and plans workgroup, one of seven formed after the multi-agency May 7, 2004, MDA summit, developed seven essential tasks that, when accomplished, are expected to achieve comprehensive Maritime Domain Awareness. These tasks include monitoring of vessels, people, cargo, and designated areas of interest in the global maritime environment; accessing all relevant databases; collecting, analyzing, disseminating relevant information; and developing appropriate metrics to measure performance toward accomplishment of the MDA related missions.

The other workgroups included ones for technology, legal, intelligence, common operational picture, outreach and budget. The intelligence workgroup defined the potential threats and the technology work group initiated a survey of what assets were available within the government to assist in the detection of those threats. Once it was understood what the agreed tasks were versus those threats, and a rough idea of what concept of operations was feasible and likely to be enacted, the technology workgroup performed a gap analysis on the entire MDA system and proposed a range of initiatives to improve the capability to detect, track, classify, and identify vessels, the cargo in them and the people on them, including their intentions, in the Technology Roadmap.

Technological Solutions

Since a core requirement of the MDA collaborative information environment is accurate vessel detection

and location data, the technology workgroup examination focused on ways to enhance the ability to detect vessels and craft both on the high seas and in the littorals. They looked at both sensors and likely platforms.

Radar

The first area of examination was, not surprisingly, long range radar systems upgrades. The utility of three types of long range (beyond line of sight) high frequency radars is being studied:

- The buoy-mounted HF surface wave radar, currently used for ocean current and wave height observation, appears to have promise. This is especially true if several are used together in a multi-static mode.
- The very large array relocatable over the horizon radar (ROTHR) appears the most promising in many ways, with demonstrated detection ranges of 1500+ miles.
- The large array shore or barge-based HF surface way radar, which may have some limited utility in unpopulated areas.

Other sensors

To screen shipments before they depart foreign countries destined for the United States, Customs and Border Protection (CBP) uses non-intrusive technology to quickly inspect cargo containers. Enhanced capability to detect a wider variety of potentially threatening substances is under development. Additionally, smart boxes, which are shipping containers with built-in sensors that can detect temperature changes or unauthorized entry and some prohibited items, now in use to protect valuable or perishable contents, are currently being evaluated.

New sensors— both active, such as upgraded radars, and passive, such as the exploitation of the reflection of radio, TV, cell tower and satellite downlink signals, and acoustics—are being examined.

Formation of the National Strategy for Maritime Security

Today, a major paradigm shift is occurring with regard to Maritime Domain Awareness, as the Coast Guard, in active partnership with a broad range of governmental agencies, seeks to protect U.S. ports and waterways from those who would do them harm.

Indeed, since September 11, 2001, numerous war games, seminars, and forums have been held to discuss needed improvements in the maritime security of the United States. Those discussions ranged from the search for technological silver bullets to legal and policy issues, to resources required gathering and analyzing all forms of intelligence and information. In August 2003, the U.S. Coast Guard, the lead federal agency for security in the Maritime Domain, recognized its lead responsibility and created the Maritime Domain Program Integration Office (MDA PIO).

It was immediately recognized that there needed to be a summit of all federal agencies involved in the Maritime Domain, and, beginning in January 2004, planning was initiated. The MDA summit concept plan was quickly approved by the Secretaries of Defense and of Homeland Security. Over the next four months, numerous planning meetings were held with almost 30 federal government organizations. The culmination was the MDA Summit, held at Johns Hopkins University Applied Physics Laboratory on May 7, 2004, co-hosted by the Honorable James Loy, Deputy Secretary for Homeland Security, and the Honorable Paul McHale, Assistant Secretary of Defense for Homeland Defense. In attendance were senior members of every federal agency with a stake in the U.S. Maritime Domain.

Due to meticulous pre-planning, the senior members of those 25+ agencies were able to agree on just what MDA is, establish its guiding principles, achieve a baseline understanding of the issues involved, and set a course for the way ahead. One of the main findings was that the efforts to provide the maritime security of the United States was heretofore disjointed and lacked clear authority and chain of command. To address this challenge, a senior steering group, made up of deputy cabinet level members, was created, and a team, co-led by the Navy and the Coast Guard, was formed to develop an implementation plan and draft a presidential directive.

An accepted definition of MDA was agreed upon: "The effective understanding of anything associated with the global Maritime Domain that could impact the security, safety, economy, or environment of the United States." This is an extremely broad and ambitious definition, which by its breadth requires unprecedented levels of cooperation among U.S. government agencies, civil authorities, foreign government agencies, and private industry. That cooperative effort is reflected in the broad composition and subject matter of the seven workgroups that were established to address various aspects of MDA. Those workgroups included strategy and plans, legal, outreach, budget and resources, intelligence, common operational picture, and technology.

On December 21, 2004, President George W. Bush signed the National Security Presidential Directive-41/Homeland Security Presidential Directive-13. This dual-titled directive established U.S. maritime security policy and directed the development of a wide-ranging National Strategy for Maritime Security (NSMS) that includes eight policy actions. The NSMS was subsequently signed on September 20, 2005. The eight supporting plans followed suit over the next several months.

The purpose of the directives is to enhance U.S. national security by focusing the disparate maritime security-related efforts occurring across a wide range of government agencies into a cohesive and comprehensive national effort. The first, and most fundamental, of the policy actions is Maritime Domain Awareness. Each policy action has a deliverable due to the president, and, in the case of MDA, this deliverable is a national plan to achieve Maritime Domain Awareness.

To that end the MDA Implementation Team has been created and is now at work.

Platforms
Commercial satellites, and high and medium altitude, long endurance craft, both lighter-than-air and more conventional unmanned aircraft such as the Global Hawk, have the potential to localize and identify vessels on the high seas. Unconventional platforms, such as lighter-than-air vehicles (free-floating and tethered), oceanic surveillance buoys, and new buoys built for ship surveillance, are being considered for surveillance of our approaches. Employing existing oil rigs or even building new, free-floating platforms for surveillance purposes are also under consideration. Nothing is off the table.

Transponders/Beacons
Large commercial vessels now carry a collision avoidance and harbor traffic control device called the automatic identification system (AIS). It contains information similar to the transponders carried on airliners, and work is underway to convert this system to a system similar to air traffic control, to better identify all vessels near U.S. shores. Eventually, AIS may have space-based relays on commercial satellites. These same ships are also required to carry the satellite communication-based Global Maritime Distress and Safety System (GMDSS) which can be polled to determine the ship's location. Additionally, several companies now sell commercial satellite-based asset tracking systems which could also be used as a vessel tracking system at a nominal cost. Both the U.S. Air Force and the U.S. Army are using commercial satellite-based systems for asset and "blue force tracking" to good effect. Expansion of either, or both, for use as an MDA tool is under consideration.

Operational Concept
Coupling long range sensors with cooperative reporting devices, such as AIS, and satellite-based tracking devices, with the mandated advanced notice of arrival—which requires all large commercial vessels to report their intention of entering a U.S. port 96 hours in advance—appears to best establish a baseline as to what is approaching the U.S. coast. Sensors, as described above, coupled with the transponder/beacon systems, could determine which contacts are not reporting, thereby allowing watchstanders and analysts could focus special attention of those few tracks. One of the first things they would do is query data bases to understand known potential problems. A description of some of the tools under consideration is below.

Data Fusion
Another rich area for the development of understanding of MDA's environment is data fusion including, data-mining, pattern recognition and anomaly detection of information in existing databases, owned by a wide range of organizations, including many governmental organizations, international organizations, and cooperative private companies such as insurance, trading, shipping, and ship building and operating companies who fully understand it is in everyone's best interest to participate in the CIE. Analytical software that can either run alone, or in conjunction with data-mining and anomaly detection software, is being developed.

A Look to the Future
Global information system display and decision tools for analysis and decision makers at all levels are also being investigated, as are the means to tie all of these functions together and build a true, real-time, common operational picture. One of the major initiatives in this area is composable FORCENet, which allows the user to define his/her relevant community of interest on the fly. Composable FORCENet, a Navy initiative to build its own service-oriented architecture (SOA), is developing the tools to allow a user to quickly define his own rules for his own information domain, using smart push and pull tools to make optimum use of all information available and relevant to the particular system/console operator. It will build the user defined operational picture.

Great strides can be made toward improving Maritime Domain Awareness through efforts to enable and enhance information sharing among governmental agencies and by incentivizing private industry participation. However, there are significant policy as well as technological challenges to be overcome. Notable synergies will be realized, as various operational pictures are integrated and databases from participating agencies are made available.

Beyond establishing communication pathways, policy, as well as technical, solutions are also being sought to solve issues concerning restricted data accessibility and protection of civil liberties and proprietary information. If anything, the policy issue is actually larger than the technology issues. Much has been done, but more remains to be done. The Navy /Coast Guard team, working together, is fully engaged in developing new ways to safeguard the United States from a wide range of possible maritime threats.

About the author: *Mr. George Guy Thomas is Science & Technology Advisor, Maritime Domain Awareness, U.S. Coast Guard. A retired Navy commander, he has published several articles on technical intelligence, reconnaissance and surveillance systems, and electronic warfare. Mr. Thomas is a distinguished graduate of the Naval War College, he holds a Master's Degree in Computer Information Systems from Bryant College. He is a member of Delta Mu Delta, national graduate school honor society.*